

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION**

ENTRI, LLC,

Plaintiff,

vs.

GODADDY.COM, LLC,

Defendant.

Case No. 1:24-cv-00569-AJT-WEF

**DEFENDANT GODADDY.COM, LLC'S OPPOSITION TO ENTRI LLC'S
MOTION TO DISMISS GODADDY.COM LLC'S SECOND
AND THIRD COUNTERCLAIMS**

TABLE OF CONTENTS

| | | |
|------|---|----|
| I. | INTRODUCTION | 1 |
| II. | BACKGROUND | 2 |
| A. | GoDaddy Registers Domain Names and Provides Services to Configure Settings | 2 |
| B. | GoDaddy Offers DNS Configuration Services to Integrate SaaS Software | 3 |
| C. | GoDaddy’s Brief Partnership with Entri..... | 4 |
| D. | Entri Continues to Unlawfully Access GoDaddy’s Software and Systems | 5 |
| III. | ARGUMENT | 7 |
| A. | GoDaddy Sufficiently Pled Breach of GoDaddy’s API TOU | 7 |
| 1. | The API TOU is an Enforceable Contract | 8 |
| 2. | Entri Breached the API TOU | 12 |
| 3. | GoDaddy was Damaged by Entri’s Breach of the API TOU | 14 |
| B. | GoDaddy Sufficiently Pled Violation of the Computer Fraud and Abuse Act..... | 18 |
| 1. | Entri’s Access was Not Authorized | 20 |
| 2. | Entri Obtained Information from a Protected Computer | 24 |
| 3. | GoDaddy Sufficiently Pled Damages | 26 |
| IV. | CONCLUSION..... | 30 |

TABLE OF AUTHORITIES

| | Page(s) |
|---|---------|
| <u>Cases</u> | |
| <i>A.V. ex rel. Vanderhye v. iParadigms, LLC</i> , 562 F.3d 630 (4th Cir. 2009) | 21, 28 |
| <i>Am. Online, Inc. v. LCGM, Inc.</i> , 46 F. Supp. 2d 444 (E.D. Va. 1998) | 24 |
| <i>AvePoint, Inc. v. Power Tools, Inc.</i> , 981 F. Supp. 2d 496 (W.D. Va. 2013) | passim |
| <i>Bell Atlantic Corp. v. Twombly</i> , 550 U.S. 544 (2007) | 18 |
| <i>Bellefonte Re Ins. Co. v. Argonaut Ins. Co.</i> , 757 F.2d 523 (2d Cir.1985) | 14 |
| <i>Civic Center Motors, Ltd. v. Mason Street Import Cars, Ltd.</i> , 387 F. Supp. 2d 378 (S.D.N.Y. 2005) | 29 |
| <i>Compass iTech, LLC v. eVestment All., LLC</i> , 2016 WL 10519027 (S.D. Fla. June 24, 2016) | 21 |
| <i>Concepts, Inc. v. Mountain Corp.</i> , 2012 WL 6761880 (W.D. Va. Dec. 30, 2012) | 11 |
| <i>CoStar Grp., Inc. v. Leon Cap. Grp., LLC</i> , 2023 WL 5133182 (D.D.C. Aug. 10, 2023) | 29 |
| <i>CoStar Realty Info., Inc. v. Field</i> , 612 F. Supp. 2d 660 (D. Md. 2009) | 20 |
| <i>Cvent, Inc. v. Eventbrite, Inc.</i> , 739 F. Supp. 2d 927 (E.D. Va. 2010) | 8, 9 |
| <i>Estes Forwarding Worldwide LLC v. Cuellar</i> , 239 F. Supp. 3d 918 (E.D. Va. 2017) | 20 |
| <i>Facebook, Inc. v. Power Ventures, Inc.</i> , 844 F.3d 1058 (9th Cir. 2016) | 25, 30 |
| <i>Farmers Ins. Exch. v. Auto Club Grp.</i> , 823 F. Supp. 2d 847 (N.D. Ill. 2011) | 27 |
| <i>Fla. Atl. Univ. Bd. of Trustees v. Parsont</i> , 465 F. Supp. 3d 1279 (S.D. Fla. 2020) | 24 |
| <i>Foster v. Walmart, Inc.</i> , 15 F.4th 860 (8th Cir. 2021) | 10 |
| <i>Good 'Nuff Garage, LLC v. McCull</i> , 2022 WL 4485810 (E.D. Va. 2022) | 25, 26 |
| <i>Job v. Simply Wireless, Inc.</i> , 160 F. Supp. 3d 891 (E.D. Va. 2015) | 17 |
| <i>Lovinfosse v. Lowe's Home Centers, LLP</i> , 2024 WL 3732436 (E.D. Va. Aug. 8, 2024) | 8, 9 |
| <i>Microsoft Corp. v. Does 1-2</i> , 2022 WL 18359421 (E.D. Va. Dec. 27, 2022) | 26 |

| | |
|---|----------------|
| <i>Microsoft Corp. v. Does</i> , 2020 WL 13894281 (E.D. Va. Nov. 20, 2020)..... | 28 |
| <i>Microsoft Corp. v. John Does 1-8</i> , 2015 WL 4937441 (E.D. Va. Aug. 17, 2015)..... | 26 |
| <i>Nguyen v. Barnes & Noble Inc.</i> , 763 F.3d 1171 (9th Cir. 2014) | 10 |
| <i>O'Neil & Assocs., Inc.</i> , 708 F. Supp. 2d 669 (N.D. Ohio 2010)..... | 21 |
| <i>Osborne v. American Multi Cinema, Inc.</i> , 348 F. App'x 535 (11th Cir. 2009) | 23 |
| <i>Patrick Patterson Custom Homes, Inc. v. Bach</i> , 586 F. Supp. 2d 1036 (N.D. Ill. 2008) | 30 |
| <i>Phoenix Co., Inc. v. Castro-Badillo</i> , 2024 WL 3742368 (D.P.R. Aug. 9, 2024)..... | 29 |
| <i>Phreesia, Inc. v. Certify Glob., Inc.</i> , 2022 WL 911207 (D. Md. Mar. 29, 2022)..... | 22 |
| <i>Precision Franchising, LLC v. T&S Holdings, Inc.</i> , 2024 WL 4329115 (E.D. Va. Mar. 1, 2024)..... | 16 |
| <i>Princess Cruises, Inc. v. Gen. Elec. Co.</i> , 143 F.3d 828 (4th Cir.1998) | 8 |
| <i>Real Time Medical Systems, Inc. v. PointClickCare Technologies, Inc.</i> , 2024 WL 3569493 (D. Md. July 29, 2024)..... | 17 |
| <i>Register.com, Inc. v. Verio, Inc.</i> , 356 F.3d 393 (2d Cir. 2004)..... | 10, 11 |
| <i>Space Sys./Loral, LLC v. Orbital ATK, Inc.</i> , 306 F. Supp. 3d 845 (E.D. Va. 2018) | 20, 28 |
| <i>State Analysis, Inc. v. Am. Fin. Servs. Assoc.</i> , 621 F. Supp. 2d 309 (E.D. Va. 2009) | 21, 22 |
| <i>Sun . Braddock Place Townhouse Assoc. ,</i> 2020 WL 4572916 (E.D. Va. Aug. 7, 2020)..... | 11 |
| <i>White Oak Power Constructors v. Mitsubishi Hitachi Power Sys. Ams., Inc.</i> , 2019 WL 3752961 (E.D. Va. Aug. 8, 2019)..... | 14 |
| <i>Student A v. Liberty Univ., Inc.</i> , 602 F. Supp. 3d 90911 (W.D. Va. 2022) | 17 |
| <i>Sunrise Continuing Care, LLC v. Wright</i> , 277 Va. 148 (2009) | 14 |
| <i>Sw. Airlines Co. v. BoardFirst, L.L.C.</i> , 2007 WL 4823761 (N.D. Tex. Sept. 12, 2007)..... | 9, 10, 12, 13 |
| <i>Tax Int'l, LLC v. Kilburn & Assocs., LLC</i> , 157 F. Supp. 3d 471 (E.D. Va. 2016) | 7, 14 |
| <i>Ticketmaster L.L.C. v. Prestige Ent. W., Inc.</i> 315 F. Supp. 3d 1147 (C.D. Cal. 2018) | 23, 24, 25, 26 |
| <i>William Gottlieb Mgmt. Co., LLC v. Carlin</i> , 2024 WL 1311854 (S.D.N.Y. Mar. 26, 2024) | 29 |
| <i>United States for Use & Benefit of McKenney's, Inc. v. Leebscor Servs., LLC</i> , 622 F. Supp. 3d 165 (E.D. Va. 2022) | 16 |

| | |
|---|----|
| <i>Van Buren v. United States</i> , 593 U.S. 374 (2021) | 22 |
| <i>WEC Carolina Energy Solutions LLC v. Miller</i> , 687 F.3d 199 (4th Cir. 2012) | 22 |
| <i>Worsham v. Accts. Receivable Mgmt., Inc.</i> , 497 F. App'x 274 (4th Cir. 2012) | 13 |

Statutes

| | |
|------------------------------|--------|
| 18 U.S.C. § 1030(a)(2) | passim |
|------------------------------|--------|

I. INTRODUCTION

Entri, LLC (“Entri”) claims to have developed a revolutionary software. But it has a major flaw: it requires access to GoDaddy.com, LLC’s (“GoDaddy”) systems and the data within, and use of GoDaddy’s propriety Application Programming Interface (“API”) software to work with GoDaddy domains. Rather than nurture a partnership with GoDaddy and continue its use of GoDaddy’s systems, Entri abused the parties’ relationship from the start, then made unreasonable demands when GoDaddy attempted to negotiate a fair deal after the parties’ initial agreement expired. Receiving absolutely no benefit from its partnership with Entri—but incurring significant costs—GoDaddy ended its partnership with Entri and revoked Entri’s right to access GoDaddy’s data and use its API software. But Entri did not relent. Instead, Entri devised procedures to bypass GoDaddy’s efforts to keep Entri out of its systems in knowing violation of GoDaddy’s API Terms of Use (“TOU”). It then invoked litigation to force its access.

GoDaddy brought counterclaims against Entri to recoup some of the monetary and other damages posed by Entri’s continued unauthorized use of GoDaddy’s systems. Entri now moves to dismiss two counterclaims: (1) for breach of GoDaddy’s API TOU, and (2) for violation of the Computer Fraud and Abuse Act (“CFAA”). Entri’s motion fails on both counts.

First, GoDaddy sufficiently alleged breach of its API TOU. The API TOU is a valid contract between the parties that restricts Entri’s use of GoDaddy’s proprietary API. Yet Entri violated those restrictions regardless. Entri cannot deny it is bound by GoDaddy’s API TOU while continuing to use GoDaddy’s API software, simultaneously imposing costs on GoDaddy by using that software, and, in doing so, actively and knowingly breaching the API TOU’s restrictions. Entri’s use of GoDaddy’s API damages GoDaddy by causing significant data processing costs, server costs, and security vulnerabilities.

Second, GoDaddy sufficiently alleged violation of the CFAA. Entri accessed GoDaddy's customers' settings, thus accessing GoDaddy's systems and API software, without authorization. GoDaddy made clear on numerous occasions that Entri was not permitted to access GoDaddy's systems or API. Courts routinely find lack of authorization where, as here, the defendant utilized an authorized user's login information despite knowing its own access was not authorized. Entri obtained information from GoDaddy's systems as contemplated by the CFAA when it accessed, observed, and altered the data stored within GoDaddy's systems and API. As a result, GoDaddy suffered both damages and loss in excess of \$5,000 in value, including by being forced to investigate and respond to the potential security and operational threats caused by Entri's access.

For these reasons, and the other reasons explained below, Entri's motion to dismiss should be denied. In the alternative, GoDaddy respectfully requests leave to amend its counterclaims.

II. BACKGROUND¹

A. GoDaddy Registers Domain Names and Provides Services to Configure Settings

GoDaddy is one of many domain name registrars, meaning it manages the reservation of Internet domain names registered through it by members of the public. (Dkt. 105 ¶¶ 9–11.) Specifically, for a fee and pursuant to a registration agreement, GoDaddy will associate a domain name with an accompanying IP address and make it available to the domain name system (“DNS”), thus rendering it an operational Internet address. (*Id.* ¶¶ 7–12.) Once a customer registers a domain name, the customer can then point the domain name to a website, such that anyone who navigates to that domain name will be directed to that website's location on the internet. (*Id.*)

¹ GoDaddy only includes facts relevant to its Second and Third Counterclaims, which Entri's Motion seeks to dismiss. (*See* Dkt. 140.)

GoDaddy's customers who register domain names with GoDaddy can access the settings for their domain names by logging in to GoDaddy's web portal. (*Id.* ¶ 21.) GoDaddy's systems contain its customer data, including the data its customers use to configure, or modify, their DNS settings. (*Id.* ¶¶ 21, 83, 86.) A domain registrant might configure their DNS settings if they need their website to pull and integrate information from other locations on the internet, such as third-party software from a "SaaS" company. (*Id.* ¶¶ 15–18.) For example, a domain registrant might want to display SaaS software that facilitates processing of payments on its website. (*Id.* ¶ 16.) To do so, the domain registrant would configure its DNS settings to integrate that payment application into its website so that when its website-goers use the application, the application data is properly mapped to the website. (*Id.* ¶¶ 17–18.)

GoDaddy also makes its API software available for use. API software assists with tasks such as fetching data stored on GoDaddy's systems to configure a domain registrant's DNS settings. (*Id.* ¶¶ 78–86, 110–11.) To configure DNS settings, the registrant must access data on GoDaddy's systems and, in many cases, makes use of GoDaddy's API. (*Id.* ¶¶ 24, 28, 86) Because the API is GoDaddy's proprietary software, and abuse of its API can cause significant costs and security vulnerabilities, GoDaddy has instituted the API TOU to govern the use of its API. (*Id.* ¶¶ 78–84 & Ex. 2.) Anyone who uses GoDaddy's API software agrees to be bound by the API TOU. (*Id.* ¶ 79)

B. GoDaddy Offers DNS Configuration Services to Integrate SaaS Software

For several years, to integrate SaaS software into a website, SaaS companies had to engage in a manual, labor-intensive and technical process of instructing registrants on integrating with the SaaS application for each paying registrant. (*Id.* ¶¶ 21, 23–24, 31.) This manual process caused SaaS companies to incur significant costs. (*Id.* ¶¶ 29, 31.)

In or around 2016, GoDaddy released a protocol, Domain Connect, which made it much easier for registrants to configure their DNS settings through a SaaS company's application. (*Id.* ¶¶ 19, 23, 28.) The Domain Connect protocol allowed for modification of a domain registrant's DNS settings based on a template specific to a SaaS company that was previously onboarded by GoDaddy. (*Id.* ¶ 24.) GoDaddy thereafter offered to implement the protocol for its SaaS partners. (*Id.* ¶ 26.) While use of the Domain Connect protocol benefitted SaaS companies by reducing the costs of manual configuration, the primary benefit to GoDaddy was increased opportunities with its SaaS partners. (*Id.* ¶¶ 30–31.) In fact, implementation of Domain Connect imposed costs and burdens on GoDaddy, because it had to create, process, and maintain templates and other data, and manage DNS configurations. (*Id.*) To offset these costs, GoDaddy charged fees to SaaS companies with a high number of templates and/or DNS configurations. (*Id.* ¶¶ 32–38.)

C. GoDaddy's Brief Partnership with Entri

In 2021, Entri launched Entri Connect, a program used by SaaS companies to automate the process of configuring DNS records. (*Id.* ¶¶ 39–40.) Specifically, once a SaaS company purchases and enables Entri Connect, users accessing the SaaS company's website are guided through a series of pages configured by Entri Connect to automatically update DNS records. (*Id.* ¶¶ 41–42.)

Shortly after Entri's launch, in April 2022, Entri and GoDaddy entered into a one-year Domain Connect Licensing Agreement ("License Agreement"), whereby Entri would apply its software using the Domain Connect protocol. (*Id.* ¶¶ 44–53.) Under the Agreement, Entri would send GoDaddy templates that set forth the required DNS settings for a particular SaaS company's application and GoDaddy would then onboard that template, allowing Entri Connect to configure DNS records on behalf of a SaaS company. (*Id.* ¶¶ 44–53.) The License Agreement also gave Entri authorization to use GoDaddy's API in connection with its services. (*Id.* ¶ 103.)

Entri's demands to onboard templates far exceeded those of any of GoDaddy's other partners, [REDACTED] (*Id.* ¶¶ 46–49.) In other words, Entri would charge its customers to use its services but then request free services from GoDaddy, while GoDaddy incurred costs with no ability to recoup them. (*Id.* ¶ 53.)

After the License Agreement expired on April 7, 2023, GoDaddy and Entri engaged in discussions regarding a continued business relationship and licensing agreement. (*Id.* ¶ 62.) Entri aggressively pushed GoDaddy for various concessions, and the parties' negotiations fell apart in or around October 2023. (*Id.* ¶¶ 63–68.)

D. Entri Continues to Unlawfully Access GoDaddy's Software and Systems

On January 11, 2024, GoDaddy sent Entri a termination letter making clear that its license to use GoDaddy's systems to configure DNS systems had expired and that Entri's access to GoDaddy's systems was terminated. (*Id.* ¶ 70.) To stop Entri from continuing to access GoDaddy's systems and use GoDaddy's API software, GoDaddy implemented methods to disconnect Entri from its software. (*Id.* ¶¶ 77–84.)

In or around February 2024, GoDaddy updated its DNS configuration system, Domain Connect, which continued to be based on the Domain Connect open standard protocol GoDaddy had helped to create years prior. (*Id.* ¶¶ 73–74.) Unlike in prior years, GoDaddy decided to charge universal fees for its services. (*Id.* ¶¶ 74–76.) This allowed GoDaddy to continue offering its SaaS partners the benefit of easier and more cost-effective domain configuration services while also allowing GoDaddy to recoup some of the costs it had been incurring without compensation. (*Id.*)

Nonetheless, despite the license agreement being terminated and GoDaddy's explicit statement that Entri's access rights were terminated, Entri continued to improperly impose costs on GoDaddy, while collecting payment from Entri's SaaS company customers. Apparently figuring out how to circumvent to GoDaddy's efforts to block Entri from its systems, Entri was

continuing to collect GoDaddy's customer login information and configure their DNS settings. (*Id.* ¶¶ 77, 86.) In doing so, Entri was deliberately misleading GoDaddy's customers into thinking that they are logging onto a legitimate and authorized GoDaddy platform, while covertly presenting an Entri page that Entri designed to harvest their GoDaddy credentials. (*Id.* ¶¶ 87–92.) Indeed, Entri designed its user login portal in a way that mimics GoDaddy's own login credential page and references GoDaddy's name and intellectual property. (*Id.* ¶¶ 88–89.)

As GoDaddy investigated Entri's unauthorized access to GoDaddy's systems and API, all while incurring continued costs of Entri's numerous API calls, on March 1, 2024, GoDaddy updated its API TOU to make clear that Entri was prohibited from using GoDaddy's API to configure DNS settings. (*Id.* ¶ 72.) GoDaddy then reiterated to Entri the restriction against Entri's use of GoDaddy's API and that Entri's conduct violated those terms. (*Id.* at 24 ¶ 199; *id.* ¶¶ 80–83.)

Nonetheless, Entri continued to use the improperly obtained GoDaddy customer credentials to access GoDaddy's systems and API in direct violation of GoDaddy's demand that Entri cease its conduct and of the API TOU. (*Id.* ¶¶ 82–86.) Entri's API requests directed at GoDaddy's systems impose significant data processing and server costs on GoDaddy. (*Id.* ¶¶ 82–92.)

Entri's conduct also creates significant security vulnerabilities because Entri continues to access and configure domains in a way that precludes GoDaddy's ability to monitor security threats. (*Id.* ¶ 108.) Through its access of customer settings, Entri obtains user credentials and otherwise-password-protected information by implying to users that they are inputting their credentials into a GoDaddy-protected login portal. (*Id.* ¶¶ 91–92, 112.) When Entri accesses GoDaddy's systems, it does so in a way that prevents GoDaddy's oversight and knowledge of

Entri's actions. (*Id.* ¶ 85.) As such, GoDaddy cannot prevent Entri from introducing security threats or ensure that Entri provides an adequate level of security. (*Id.*)

GoDaddy brings its counterclaims against Entri to recover some of the financial losses and other damages GoDaddy has incurred as a result of Entri's continued unauthorized access and use of GoDaddy's systems and API.

III. ARGUMENT

"[T]o survive a motion to dismiss, a Complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Tax Int'l, LLC v. Kilburn & Assocs., LLC*, 157 F. Supp. 3d 471, 475–76 (E.D. Va. 2016). "[A] claim has facial plausibility when the pleaded factual content allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* "When deciding a motion to dismiss for failure to state a claim, the court must accept as true all well-pleaded allegations and draw all reasonably factual inferences in the plaintiffs' favor." *AvePoint, Inc. v. Power Tools, Inc.*, 981 F. Supp. 2d 496, 505 (W.D. Va. 2013). "In considering a Rule 12(b)(6) motion, the court may properly consider exhibits attached to the complaint in addition to the complaint itself." *Id.* at 505–06.

A. GoDaddy Sufficiently Pled Breach of GoDaddy's API TOU

GoDaddy alleges that Entri breached its API TOU by using GoDaddy's proprietary API software for commercial gain despite knowing that GoDaddy's API TOU prohibited such use. To state a claim for breach of contract, GoDaddy must allege: "(1) a legally enforceable obligation of a defendant to a plaintiff; (2) the defendant's violation or breach of that obligation; and (3) injury or damage to the plaintiff caused by the breach of obligation." *Id.* at 509. GoDaddy has sufficiently alleged each element. Entri's Motion should be denied.

1. The API TOU is an Enforceable Contract

Entri claims that the API TOU is not an enforceable contract because GoDaddy failed to sufficiently allege mutual assent and adequate consideration. (Dkt. 140 at 7–10.) Entri misunderstands the nature of browsewrap agreements, and its arguments should be rejected.

a) *GoDaddy Alleged Mutual Assent*

Entri mischaracterizes GoDaddy’s pleadings and the law to argue that GoDaddy’s allegations are “vague and conclusory” and that Entri did not assent to the API TOU. (*Id.* at 9–10.)

“Assent may be manifested directly, by written or spoken words, or indirectly, through one’s actions or conduct.” *AvePoint*, 981 F. Supp. 2d at 509 (citing *Princess Cruises, Inc. v. Gen. Elec. Co.*, 143 F.3d 828, 834 (4th Cir.1998)). Certain “terms of use” agreements, such as “browsewrap agreement[s],”² do “not require a user to manifest assent to the terms and conditions expressly”—instead, a party “gives his assent by using the website.” *Id.* at 510. Mutual assent is found even where the party “did not bother reading the terms,” so long as there was “constructive notice of the” terms and conditions. *Lovinfosse v. Lowe’s Home Centers, LLP*, No. 1:23-cv-574, 2024 WL 3732436, at *6 (E.D. Va. Aug. 8, 2024) (cleaned up).

In arguing there was no assent, Entri primarily relies on *Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927 (E.D. Va. 2010). But in *Cvent*, the plaintiff failed to allege that the defendant had any knowledge of the terms and conditions, whether actual or constructive, instead merely

² Importantly, GoDaddy’s API TOU is actually a sign-in wrap agreement, not a browsewrap agreement, for GoDaddy’s customers because its customers must agree to the terms of use to when receiving credentials. GoDaddy’s API TOU is only a browswrap agreement *in function* for Entri because Entri circumvents the signup process by using another’s credentials. Moreover, if Entri was truly working on behalf of GoDaddy’s customers, Entri should be held to the same rules for which its customers are bound, including the API TOU.

claiming that “the terms of the TOUs [] are readily available for review.” *Id.* at 937. Here, GoDaddy alleges that Entri had both constructive and actual knowledge.

First, GoDaddy has alleged facts sufficient to show Entri had constructive knowledge. As even Entri acknowledges, GoDaddy has pled that Entri mutually assented to the API TOU, including through Entri’s use of GoDaddy’s API. (Dkt. 140 at 9 (citing Dkt. 105 ¶ 79).) Entri further acknowledges that GoDaddy pled that Entri’s use of the API was dictated by an “explicit agreement” between the parties from 2022–23 (*id.* (citing Dkt. 105 ¶ 103)), which was later terminated, showing that Entri knew that GoDaddy expected its API users to follow rules when using its software. These allegations alone show mutual assent to the API TOU. *See Lovinfosse*, 2024 WL 3732436, at *6 (finding constructive knowledge despite no knowledge of specific terms).

Second, Entri had actual knowledge of the API TOU. GoDaddy updated its API TOU on March 1, 2024, to exclude practices such as Entri’s. (Dkt. 105 ¶ 78.) On or around March 7, 2024, GoDaddy sent Entri a letter informing it of the API TOU restrictions on API use and that Entri’s conduct violated those terms. (Dkt. 105 at 24 ¶ 199; *id.* ¶¶ 80–83.) Regardless of whether Entri knew about the API TOU prior to receiving GoDaddy’s cease-and-desist letter, it certainly knew of the terms after, yet continued to breach those terms anyways. (*Id.* ¶¶ 83, 107.) Entri has been bound by the API TOU since at least that time. *See Sw. Airlines Co. v. BoardFirst, L.L.C.*, No. 3:06-CV-0891-B, 2007 WL 4823761, at *7 (N.D. Tex. Sept. 12, 2007) (defendant “had actual knowledge of” terms and conditions since receipt of “cease-and-desist letter” informing defendant “that the Terms forbid the use of [plaintiff’s] website for commercial purposes” and “bound itself to the” terms when it “continued to use [plaintiff’s] site in connection with its business”).

Entri’s conduct shows that it knew about the restrictions even before receiving GoDaddy’s letter. Entri knew that GoDaddy had “disconnect[ed] Entri from” GoDaddy’s DNS configuration

software, yet developed processes “to work around this disconnection to continue offering” its products through use of GoDaddy’s API. (Dkt. 105 ¶ 77.) That Entri went to the trouble of developing a workaround and collecting user login credentials in a misleading manner to access their user profile shows that Entri knew of restrictions prohibiting its use. *See AvePoint*, 981 F. Supp. 2d at 511 (that defendant “went to the trouble of creating a fictitious profile and email” “to download the software suggests that [it] had knowledge of the Terms and Conditions, and was aware that they prohibit users from downloading materials for commercial use”).

“[C]ourts have consistently enforced browsewrap agreements” where, like here, the user had actual notice of the agreement. *Foster v. Walmart, Inc.*, 15 F.4th 860, 864 (8th Cir. 2021) (quoting *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1176 (9th Cir. 2014)); *see also Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 402 (2d Cir. 2004) (finding likelihood of success in “breach of browsewrap” claim where defendant admitted “it continued drawing the data from [plaintiff’s] computers with full knowledge that [it] offered access subject to these restrictions”); *Sw. Airlines.*, 2007 WL 4823761, at *4–6 (finding contract formation where defendant continued breach after learning of terms by letter). And whether Entri “rejected and repudiated” the API TOU (Dkt. 140 at 9) is of no consequence.³ *See Register.com*, 356 F.3d at 402 (rejecting argument that defendant is “not bound by [] terms because it rejected them”).

b) GoDaddy Alleged Adequate Consideration

Entri alleges there was no consideration because (1) nothing in the API TOU was “of a benefit to Entri or to the detriment of GoDaddy;” and (2) “the entire purpose of the amendment was to permanently *prevent* Entri from continuing its historic practice of configuring the DNS

³ Moreover, Entri’s admission that it rejected the API TOU further underscores that Entri knew about the API TOU and choose to simply ignore it.

settings on behalf of GoDaddy customers' domains.” (Dkt. 140 at 8 (emphasis in original).) Not so. Even if the restrictions imposed on use of GoDaddy's API software prevents Entri from using the API for a specific purpose, Entri cannot use it however it wants in violation of the API TOU. Entri's commercial use of GoDaddy's API, which is governed by the API TOU, constitutes sufficient consideration. *See Cap. Concepts, Inc. v. Mountain Corp.*, No. 3:11-CV-00036, 2012 WL 6761880, at *10 (W.D. Va. Dec. 30, 2012) (access to website given “in exchange for” an agreement not “to challenge the validity of” intellectual property right was valid consideration).

Entri argues that it did not receive a benefit because the API TOU specifically prohibits Entri's desired use of the API for DNS configuration. (Dkt. 140 at 8.) But courts routinely uphold restrictions on software use, even when such restrictions limit the commercial purpose of the user of that software. *See, e.g., AvePoint*, 981 F. Supp. 2d at 510–11 (defendant bound to terms of use restrictions on downloading software for “commercial use” where it had knowledge of terms and used software); *Register.com*, 356 F.3d at 401 (defendant was bound to terms prohibiting use of registrar list for commercial purposes despite only wanting list for commercial purposes). These cases illustrate that the enforceability of such terms does not hinge on the user's subjective benefit but rather on the mutual obligations established. Entri's cited case, *Sun v. Braddock Place Townhouse Assoc.*, does not hold otherwise. No. 1:19-cv-00423, 2020 WL 4572916, at *5 (E.D. Va. Aug. 7, 2020) (providing a legally mandated disclosure was not consideration because it conferred no additional benefit beyond what the law required). In contrast, Entri's use of GoDaddy's API software is not a legal obligation but a privilege granted under specific terms, which Entri accepted and from which it derived substantial benefit. Therefore, Entri cannot disregard the API TOU simply because it disagrees with its restrictions. The mutual exchange—the provision of API access by GoDaddy and the adherence to usage limitations by Entri—

constitutes valid consideration, rendering the API TOU enforceable.

2. Entri Breached the API TOU

Rather than dispute that it engaged in the conduct prohibited by the API TOU, Entri argues that it did not breach the API TOU because it is not the “user” that the API TOU restricts. (Dkt. 140 at 10.) Entri’s argument is not credible.

The API TOU sets forth rules relating to “Access [and] Usage” of GoDaddy’s API. (Dkt. 105, Ex. 2.) Under the API TOU, “Users” of the API are prohibited from “register[ing], transfer[ring], renew[ing], or modify[ing] domains or products that are not under the user’s direct control.” (*Id.* ¶ 80 & Ex. 2.) “Users or other entities” are also prohibited from “charg[ing] any fees, requir[ing] any payment or compensation, or otherwise offer[ing] a service behind a paywall that uses any part of the GoDaddy API or offer[ing] any services or products that use or rely on the GoDaddy API, including any services or products offered to users by third parties.” (*Id.* ¶ 81 & Ex. 2) Entri was bound by those terms and breached them when it used the API for its commercial gain.

The decision in *Southwest Airlines Co. v. BoardFirst, L.L.C.* is on point. 2007 WL 4823761. In that case, Southwest Airlines passengers authorized BoardFirst to log into their accounts and check them into their flights for first-come-first-serve-style priority boarding. *Id.* at *1. The Court granted summary judgment in favor of Southwest for BoardFirst’s breach of Southwest’s terms of use, which prohibited commercial use of Southwest websites by third parties, because BoardFirst was aware of the terms of use at least since it received Southwest’s cease-and-desist letter and continued to use Southwest’s website in breach of the terms. *Id.* at *4–5. The Court explicitly rejected BoardFirst’s argument that it was acting as an authorized agent on behalf of the passengers, reasoning that their authorization did not “make [BoardFirst’s] conduct any less

of a violation of the Terms.” *Id.* at *7. The Court further rejected BoardFirst’s argument that the term “third party” is “ambiguous because it is undefined,” as it was “evident [that the] overriding aim [of the terms was] to prevent the Southwest site from being used for commercial purposes.” *Id.* (finding BoardFirst’s “use of southwest.com” “[p]lainly” violates Southwest’s terms of use).

Similarly, here, the API TOU was plainly intended to restrict Entri’s use of the API, and Entri knew of those restrictions, yet Entri continued to use the API in violation of its terms. (Dkt. 105 ¶¶ 77–86, 104–107.) Specifically, once contract negotiations to continue the parties’ partnership broke down, GoDaddy disconnected Entri from its Domain Connect product. (*Id.* ¶¶ 63–70.) Then, upon learning that Entri had managed “to work around this disconnection to continue offering DNS configuration to GoDaddy’s end users,” GoDaddy updated its API TOU “to address Entri’s abuse of its API.” (*Id.* ¶¶ 63–64, 77–78.) Despite GoDaddy’s efforts, Entri “used GoDaddy customer[s]’ credentials” to log into their accounts, then used GoDaddy’s API “in furtherance of Entri’s commercial activities” (*id.* ¶ 86), such as “offer[ing] its paid product and service, Entri Connect, to third parties” and “access[ing] GoDaddy’s API to modify data associated with those user accounts.” (*Id.* ¶¶ 105–07.) Entri’s actions are in direct violation of the API TOU. (*Id.* ¶¶ 105–07.) “That [Entri] is authorized to do so by [GoDaddy’s] customers does not make its conduct any less of a violation of the Terms.” *See Sw. Airlines*, 2007 WL 4823761, at *7.

Entri’s argument is also contradicted by its own claims. Entri argued in its Motion that “the entire purpose of the [API TOU] amendment was to permanently prevent Entri from continuing its historic practice of configuring the DNS settings.” (Dkt. 140 at 8.) Entri also alleged in its Complaint that Entri “perform[s] the domain integration”⁴ (Dkt. 23 ¶ 66), and that GoDaddy

⁴ “A party’s assertion of fact in a pleading is a judicial admission by which it normally is bound throughout the course of the proceeding.” *Worsham v. Accts. Receivable Mgmt., Inc.*, 497 F. (Continued...)

intended the API TOU to prevent Entri’s use of its API and believed that Entri’s use of GoDaddy’s API violated the API TOU. (*Id.* ¶ 181.) Entri cannot argue that the API TOU prevents its conduct but then, in the same breath, argue that it is not the one restricted by the API TOU.

In any event, the term “users” is not ambiguous. The term is used in a section dictating “API Access[and] Usage,” and the API TOU states that it binds anyone who “us[es] the GoDaddy API.” (Dkt. 105, Ex. 2.) Common sense dictates that “user” refers to those who use or access GoDaddy’s API. *See Tax Int’l*, 157 F. Supp. 3d at 476 (“Assessing the claim is a context-specific task that requires the reviewing court to draw on its judicial experience and common sense.”); *White Oak Power Constructors v. Mitsubishi Hitachi Power Sys. Ams., Inc.*, No. 3:17-cv-00355-JAG, 2019 WL 3752961, at *3 (E.D. Va. Aug. 8, 2019) (“[A] court should not shy away from searching for the unambiguous, plain meaning of the text.”). GoDaddy thus sufficiently alleged that Entri breached the API TOU.

3. GoDaddy was Damaged by Entri’s Breach of the API TOU

Entri—quoting caselaw describing the adequacy of evidence presented at trial to support a jury verdict—argues that GoDaddy does not allege “damages with the requisite specificity.” (Dkt. 140 at 11 (citing *Sunrise Continuing Care, LLC v. Wright*, 277 Va. 148, 156 (2009).) GoDaddy alleged sufficient damages to defeat a Rule 12(b)(6) motion.

For example, as even Entri acknowledges in its brief, GoDaddy alleged that Entri’s breach caused “‘significant data processing and server costs’” through Entri’s significant number of calls to GoDaddy’s API software and “creation of ‘security vulnerabilities by allowing Entri Connect to access and configure domains without GoDaddy oversight.’” (*Id.* (quoting Dkt. 105 ¶ 108).)

App’x 274, 277 (4th Cir. 2012) (quoting *Bellefonte Re Ins. Co. v. Argonaut Ins. Co.*, 757 F.2d 523, 528 (2d Cir.1985)).

To put GoDaddy’s damages in context, to integrate a SaaS platform, SaaS companies have to either (1) engage in a “labor-intensive and technical [process] of instructing registrants on integrating with the SaaS application” for each paying website registrant, which does not require processing of templates and was of little cost to GoDaddy (Dkt. 105 ¶¶ 23–24, 31); or (2) adopt GoDaddy’s Domain Connect protocol, which imposed costs on GoDaddy due to the processing of templates and managing DNS configurations. (*Id.* ¶¶ 32–36.) Historically, GoDaddy offset those costs by charging fees to SaaS companies with a high number of templates and/or DNS configurations. (*Id.* ¶¶ 32–38.)

Entri, however, is imposing on GoDaddy significant data processing and server costs (*id.* ¶ 84)—including through numerous requests directed at GoDaddy’s proprietary API software—and at a rate many times higher than GoDaddy’s SaaS partners and with no payment to GoDaddy to offset these costs. (*Id.* ¶¶ 64, 83.) Without any contract between the parties to compensate GoDaddy for Entri’s use of its API,

[Entri is] profiting off GoDaddy’s free support: . . . Entri [is] offer[ing] its own DNS configuration service, Entri Connect, for use in connection with domains registered with GoDaddy, and Entri [is] charg[ing] service providers for such use [while imposing costs on GoDaddy]. . . . This compensation imbalance harm[s] GoDaddy financially and operationally.

(*Id.* ¶¶ 53–54.) Entri also introduces serious security risks to (1) GoDaddy’s customers through its open access to their credentials, API keys (i.e., the “keys” to their website), and (2) GoDaddy’s ability to confirm to its consumers that they are logging in to a secure platform that GoDaddy then has to spend significant time and resources trying to overcome. (*Id.* ¶¶ 91–92). Indeed, Entri gives GoDaddy’s customers the illusion that they are inputting their credentials into a GoDaddy-protected login portal. (*Id.*) When Entri uses GoDaddy’s API software without any oversight by GoDaddy, GoDaddy has no way of preventing Entri from introducing security threats or ensuring

that Entri is providing adequate security to GoDaddy’s customers. (*Id.* ¶ 85.)

GoDaddy’s damages are far from conclusory, or vague, and are sufficient to defeat a motion to dismiss. *See AvePoint*, 981 F. Supp. 2d at 509–11 (“allegations” of “direct and consequential damages as a result of the breach” were “arguably conclusory” but “sufficient . . . to permit the court to reasonably infer” the damages element could “be met”).

Relying on inapposite case law regarding the adequacy of proof as to causation at trial, Entri also argues that GoDaddy failed to “establish[] a causal connection between [Entri’s] breach and the damages claimed” because GoDaddy’s damages were “ordinary operating costs that would have been incurred absent Entri’s alleged conduct.” (Dkt. 140 at 11–12 (quoting *United States for Use & Benefit of McKenney’s, Inc. v. Leebcor Servs., LLC*, 622 F. Supp. 3d 165, 176 (E.D. Va. 2022) (failing to prove damages were caused by counterparty and not itself)). Not so. Entri’s “API requests directed at GoDaddy’s systems . . . impose significant data processing and server costs on GoDaddy” without “compensation to offset these costs.” (Dkt. 105 ¶¶ 83–92.) As explained above, absent Entri’s breach, GoDaddy either would not have incurred the same costs (if no DNS protocol were used) or could have recouped its costs from SaaS companies. And it would not have expended time and resources on addressing security risks. When Entri uses GoDaddy’s API instead of Domain Connect, GoDaddy incurs costs and has no ability to recoup them.

Finally, Entri contends that GoDaddy has not adequately alleged damages to survive a motion to dismiss, relying on a report and recommendation for approval of a motion for default judgment. (Dkt. 140 at 12 (quoting *Precision Franchising, LLC v. T&S Holdings, Inc.*, No. 1:23-cv-858 RDA/IDD, 2024 WL 4329115, at *3 (E.D. Va. Mar. 1, 2024), for the principle that damages must be “prove[n] [] with reasonable certainty”). As discussed above, the security vulnerabilities

and costs imposed by Entri’s use of GoDaddy’s API are concrete damages sufficient to survive a motion to dismiss. *See Student A v. Liberty Univ., Inc.*, 602 F. Supp. 3d 901, 911 (W.D. Va. 2022) (holding that where “Plaintiffs have identified in their amended complaint all the material terms of the contract that they allege they concluded with [defendant] and that [defendant] purportedly breached, and that they suffered economic damages as a result,” then “no more is required.”); *Job v. Simply Wireless, Inc.*, 160 F. Supp. 3d 891, 900 n.10 (E.D. Va. 2015) (explaining that “at the motion to dismiss stage[,] the general allegation that plaintiffs have suffered damage is sufficient for the claim to survive”).

Entri mischaracterizes GoDaddy’s claims when it argues that GoDaddy previously permitted Entri to configure services without security vulnerabilities. (Dkt. 140 at 12 (citing Dkt. 105 ¶¶ 41–42).) GoDaddy entered into a licensing agreement with Entri shortly after Entri’s launch. (Dkt. 105 ¶¶ 39–45 & Ex. 1.) Now, having no partnership with Entri, GoDaddy lacks any oversight. (*Id.* ¶ 85.) GoDaddy need not plead that a specific “security incident [] has occurred” to survive a motion to dismiss; it needs only to plausibly allege that it has suffered damages. (Dkt. 140 at 12.)⁵

GoDaddy’s counterclaims “contain[] sufficient factual content to permit the court to reasonably infer that” GoDaddy incurred damages. *AvePoint*, 981 F. Supp. 2d at 511 (holding Rule 12(b)(6) dismissal of claims based on browsewrap agreement “would be premature” where “arguably conclusory” damages were sufficient to infer all elements met).

* * *

⁵ Entri mischaracterizes the one case it cites in support of its argument, *Real Time Medical Systems, Inc. v. PointClickCare Technologies, Inc.*, No. 8:24-cv-00313-PX, 2024 WL 3569493, at *3 n. 2 (D. Md. July 29, 2024). (*See* Dkt. 140 at 13.) That case does not support Entri’s argument. *Real Time Medical Systems* only discussed security risks in a description in the background section. 2024 WL 3569493, at *3. It did not “reject[]”—or even address—any “arguments” relating to any “security risks” or damages as Entri claims.

GoDaddy's claims are not the type of "formulaic recitation of the elements of a cause of action" prohibited by *Twombly*. See *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007). "Under the standard of *Iqbal* and *Twombly*, [GoDaddy] has adequately alleged that" Entri knew of the API TOU and thus was bound by its terms; Entri breached those terms by using the API; "and that [GoDaddy] was damaged by that act. That represents all the elements for breach of contract under Virginia law. [] Therefore, [Entri's] motion to dismiss [GoDaddy's] breach of contract claim will be denied." *Trustees of Hackberry Baptist Church v. Womack*, 62 F. Supp. 3d 523, 530 (W.D. Va. 2014). See also *AvePoint*, 981 F. Supp. 2d at 511 ("[D]eclaring the browsewrap agreement unenforceable under Rule 12(b)(6) would be premature [because the] complaint contains sufficient factual content to permit the court to reasonably infer that all of the required breach of contract elements can be met.").

B. GoDaddy Sufficiently Pled Violation of the Computer Fraud and Abuse Act

Entri challenges nearly every element of GoDaddy's CFAA claim. (Dkt. 140 at 13–22.) Entri's motion should be denied.

As an initial matter, Entri argues that GoDaddy does not identify a specific subsection of 18 U.S.C. § 1030 that Entri violated. GoDaddy has successfully pled a claim pursuant to subsection (g), subsection (a)(2)(C), subsection (a)(5)(C), and subsection (c)(4)(A)(i). Subsection (g) allows a party to bring a civil suit for "compensatory damages" or "equitable relief" if that person "suffers damage or loss by reason of a violation of [Section 1030]." Under Subsection (a)(2)(C), whoever (1) "intentionally accesses a computer"; (2) "without authorization or exceeds authorization access"; and (3) "thereby obtains . . . information from any protected computer" violates the Section. Subsection (a)(5)(C) is similar, but without the information requirement, and imposes liability on whoever (1) "intentionally accesses a protected computer"; (2) "without

authorization,” and (3) “as a result of such conduct, causes damage and loss.” Under both subsections, the conduct must also involve one “of the factors set forth” in subsection (c)(4)(A)(i) (18 U.S.C. § 1030(g)), none of which are relevant here except factor (I): “loss to 1 or more persons during any 1-year period . . . aggregating at least \$5,000 in value.” GoDaddy’s allegations plainly allege elements of these subsections.

GoDaddy alleges that: *First*, Entri intentionally accessed GoDaddy’s web systems and API. (Dkt. 105 ¶¶ 110–11.) *Second*, Entri’s access of GoDaddy’s systems and API was without authorization. With respect to GoDaddy’s API, once GoDaddy terminated Entri’s license to use its API, Entri’s authorization to use GoDaddy’s API was revoked. (*Id.* ¶ 110.) Yet, Entri continued to use GoDaddy’s API without authorization. (*Id.*) Entri also accessed GoDaddy’s systems without authorization by soliciting GoDaddy customer credentials in furtherance of Entri’s commercial activities and with the goal of using GoDaddy’s API. (*Id.* ¶ 111.) Entri’s solicitation of customer credentials for commercial activities was also prohibited by GoDaddy’s API TOU. (*Id.*) *Third*, Entri obtained information through its unauthorized access. Specifically, Entri obtained user credentials and procured otherwise-password-protected information within domain registrants’ settings when Entri configured their settings using data hosted in GoDaddy’s systems. (*Id.* ¶ 112.) *Fourth*, Entri’s access and use of GoDaddy’s systems and API caused GoDaddy at least \$5,000 in damages because GoDaddy was forced to “investigat[e] and respond[] to the consequences of this unauthorized access, which posed security and operational threats to GoDaddy.” (*Id.* ¶ 113.)

Indeed, GoDaddy’s allegations were sufficient for Entri to identify what subsection of the CFAA that GoDaddy claims Entri violated. (Dkt. 140 at 14 (assuming violation of Subsection 1030(g) through violation of Subsection (a)(2)(C)).) GoDaddy thus stated sufficient facts to notify

Entri as to the nature of its claims. *See Estes Forwarding Worldwide LLC v. Cuellar*, 239 F. Supp. 3d 918, 922 (E.D. Va. 2017) (denying motion to dismiss despite being “unclear as to which specific provision of the CFAA [the complaint] alleges [defendant] violated”); *Space Sys./Loral, LLC v. Orbital ATK, Inc.*, 306 F. Supp. 3d 845, 850 (E.D. Va. 2018) (denying motion to dismiss despite claimant not identifying specific CFAA provisions until “its Response”); *CoStar Realty Info., Inc. v. Field*, 612 F. Supp. 2d 660, 675 (D. Md. 2009) (denying motion to dismiss even though claimant did “not state [on] which provision of the [CFAA] the plaintiff is relying”).

1. Entri’s Access was Not Authorized

Entri misstates the law and the facts to argue that its use was authorized. As an initial matter, Entri argues that it “is not remotely guilty of felony computer hacking.” (Dkt. 140 at 14.) But GoDaddy’s “successful pleading of a CFAA violation doesn’t depend on whether [Entri] hacked anything.” *Ticketmaster L.L.C. v. Prestige Ent. W., Inc.*, 315 F. Supp. 3d 1147, 1169 (C.D. Cal. 2018) (“While . . . ‘Congress enacted the CFAA . . . primarily to address the growing problem of computer hacking,’ [] the word ‘hack’ does not appear anywhere in the statute’s text . . . [and] courts in the Ninth Circuit have repeatedly recognized violations of the CFAA without characterizing the violations as hacking.”) Entri accessed GoDaddy’s systems without authorization as contemplated by the CFAA.

Entri primarily argues that it was “authorized by GoDaddy’s customers” when it entered their login information into Entri’s “GoDaddy”-branded modal. (Dkt. 140 at 14.) Entri is wrong.

Indeed, many of GoDaddy’s allegations are premised on the fact that GoDaddy’s customers do *not* authorize Entri to use their GoDaddy login credentials. (*See, e.g.*, Dkt. 105 ¶¶ 87–91.) To be clear, GoDaddy’s customers are not Entri’s customers and do not hire Entri to help configure their websites. (*Id.* ¶ 41.) Instead, when a GoDaddy customer wants third-party functionality on

their domain, they visit the website of the entity—typically a SaaS company—that offers that functionality. Those SaaS companies are Entri’s customers. (*Id.*) When a *GoDaddy* customer goes to the website of *Entri*’s SaaS customer, they are presented with a series of screens for domain configuration that look like they come from the SaaS company. Then, they are presented with a screen that makes it look like they are logging in to GoDaddy’s platform. (*Id.* ¶¶ 87–91.) It is GoDaddy’s contention that most of its customers have no idea who Entri is and certainly have not intentionally authorized Entri—as opposed to GoDaddy or someone associated with GoDaddy—to use their GoDaddy login credentials. (*Id.* ¶¶ 88–91.) Entri’s heavy reliance in its Motion on its own interpretation of a disputed fact underscores that its Motion should be denied.

Entri’s argument is also unsupported by the law because Entri knew GoDaddy prohibited Entri’s attempts to access GoDaddy’s systems. Several “courts have held that a defendant acts ‘without authorization’” when they “use[] another’s password to access a plaintiff’s computer if the defendant had reason to believe that the password holder did not have the plaintiff’s authority to grant access to the plaintiff’s computer,” as Entri has done here. *See Compass iTech, LLC v. eVestment All., LLC*, No. 14-81241-CIV-MARRA, 2016 WL 10519027, at *2, 9 (S.D. Fla. June 24, 2016) (Compass exceeded authorization when it “used the login credentials of paying licensed users of the Analytics Database”); *see also A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 645 (4th Cir.2009) (use of another’s password to access website to submit papers without university website owner’s permission was unauthorized); *State Analysis, Inc. v. Am. Fin. Servs. Assoc.*, 621 F. Supp. 2d 309, 316 (E.D. Va. 2009) (denying motion to dismiss where former customer-turned-competitor accessed plaintiff’s website using others’ usernames and passwords where customer contracts only “authorized [*clients*] to use [plaintiff’s] subscription services”); *Snap-on Bus. Sols. Inc. v. O’Neil & Assocs., Inc.*, 708 F. Supp. 2d 669, 678 (N.D. Ohio 2010)

(denying motion for summary judgment because there was insufficient evidence that licensee “had the power to authorize any person or entity it desired[, including CFAA defendant,] to access the website and [plaintiff’s] servers”).

Entri “may not hide behind purported ‘authorization’ granted to it by [GoDaddy’s customers], particularly given that” Entri was “familiar with the terms of” GoDaddy’s API TOU, the “scope of authority granted to” GoDaddy customers, and GoDaddy explicitly told Entri it was prohibited from such use. *See State Analysis*, 621 F. Supp. 2d at 316. If it were “[o]therwise, an admittedly unwelcome computer hacker could escape liability under the CFAA by pointing to some third party who had theoretically given him permission to hack the plaintiff’s computer.” *Snap-on*, 708 F. Supp. 2d at 677–78; *Phreesia, Inc. v. Certify Glob., Inc.*, No. DLB-21-678, 2022 WL 911207, at *6 (D. Md. Mar. 29, 2022) (“[D]efendant may not hide behind purported ‘authorization’ granted to it by the client.”).

Entri also argues that “violation of a use policy does not render access unauthorized” (Dkt. 140 at 15), primarily relying on *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012) and *Van Buren v. United States*, 593 U.S. 374 (2021). But neither case held that a defendant may use another’s software in a way they know is explicitly prohibited. In both cases, the plaintiffs alleged that their employee exceeded authorization by using a work computer for personal purposes. *Van Buren*, 593 U.S. at 380–81; *WEC*, 687 F.3d at 207. Both courts held unsurprisingly that otherwise authorized employees, such as the defendants, do not exceed authorization solely by using a computer for a non-employment purpose. *See WEC*, 687 F.3d at 207 (finding liability only where employees “access computers without authorization or [] obtain or alter information beyond the bounds of their authoriz[ation]”); *Van Buren*, 593 U.S. at 396 (one “‘exceeds authorized access’ when he accesses a computer with authorization but then obtains

information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him”).⁶ Here, Entri’s conduct was never authorized, and Entri knew it.

Ticketmaster L.L.C. v. Prestige Entertainment West, Inc. is on all fours. 315 F. Supp. 3d 1147. Ticketmaster sent a letter to Prestige “explicitly prohibit[ing]” it “from using bots to access Ticketmaster’s website” to purchase tickets and informing Defendants that their use of its “website is conditioned on an agreement that” prohibits their conduct. *Id.* at 1169–71. The court held that by continuing to engage in conduct prohibited by Ticketmaster’s letter, defendants “accessed the Ticketmaster website in a manner explicitly forbidden to them, thus exceeding their authorization.” *Id.* at 1172. Unlike in *WEC* and *Van Buren*, the court reasoned that defendants were “a sophisticated multi-entity business operation, not an employee on his way out the company.” *Id.* at 1171. The court further reasoned that defendants were “commercial [entities] whose business model [was] built on unauthorized use of [Ticketmaster’s] website,” and knew that their “business model” required evasion of “Ticketmaster’s policies for profit.” *Id.* at 1170–71.

Similarly, here, Entri knew that its use of GoDaddy’s systems and API was prohibited, yet Entri continued its use in knowing violation of this prohibition. “On January 11, 2024, GoDaddy sent Entri a termination letter making clear that” its license to use GoDaddy’s systems to configure DNS systems had “expired” and that its “access” was “terminated.” (Dkt. 105 ¶ 70.) GoDaddy also informed its customers that Entri Connect was no longer allowed to be used to configure DNS

⁶ Entri cites *Osborne v. American Multi Cinema, Inc.* as a “real-world analogy” involving consumers bringing candy into a movie theater (Dkt. 140 at 16). 348 F. App’x 535 (11th Cir. 2009). Entri mischaracterizes *Osborne*, which did not involve the CFAA and does not support the proposition for which it was cited. *Id.* at 538 (upholding defendant’s summary judgment for claims of false arrest and malicious prosecution after plaintiff was banned from a movie theater, and later arrested for trespass for entering without a ticket). Entri’s analogy is inapplicable for the additional reason that GoDaddy’s customers are being tricked into providing Entri access, unlike the situation in which a consumer intentionally brings in candy in violation of the movie theater’s rules. If anything, this scenario is more akin to candy vendors sneaking into a movie theater and selling the prohibited candy to unsuspecting customers in the lobby.

records (Dkt. 105 ¶ 72), and those customers *told* Entri that GoDaddy did not want Entri configuring DNS settings. (See Dkt. 23. ¶¶ 111–16.) GoDaddy then updated its API TOU to prohibit Entri from using GoDaddy’s API (Dkt. 105 ¶ 72), and informed Entri in a second letter of the restrictions in its API TOU and that Entri’s conduct violated those terms. (*Id.* ¶¶ 80–83, *id.* at 24 ¶199.) Entri even developed a “work around [to its] disconnection to continue offering GoDaddy’s DNS configuration.” (*Id.* ¶ 77.) See *Am. Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451 (E.D. Va. 1998) (granting summary judgment where defendant used “software to evade AOL’s filtering mechanisms”).

GoDaddy alleges that Entri continued to use GoDaddy’s systems and API while knowing GoDaddy prohibited such use. That is sufficient to state a claim of unauthorized access. See *Ticketmaster*, 315 F. Supp. 3d at 1172 (exceeded authorization where committed acts prohibited by cease-and-desist letter); *Fla. Atl. Univ. Bd. of Trustees v. Parsont*, 465 F. Supp. 3d 1279, 1293 (S.D. Fla. 2020) (that defendant knew he was violating plaintiffs’ policies was “‘surefire evidence’ . . . sufficient to sustain a claim of unauthorized access”); *Am. Online.*, 46 F. Supp. 2d at 450 (granting summary judgment where defendant’s “actions violated AOL’s Terms of Service,” and thus “was unauthorized”).

2. Entri Obtained Information from a Protected Computer

Entri also argues that it did not “obtain information” in violation of Subsection (a)(2)(C). (Dkt. 140 at 17.) Violation of Subsection (a)(5)(C), however, does not require proof that information was obtained, so GoDaddy’s claim would survive even without such a showing. See 18 U.S.C.A. § 1030(a)(5)(C); *Supra* § 3b. In any event, GoDaddy sufficiently alleges that Entri obtained information in violation of Subsection (a)(2)(C). See 18 U.S.C. § 1030(a)(2)(C).

Under the CFAA, “the meaning of the words ‘obtain information’ includes not only the

copying or transporting of information, but also the mere observation, or reading, of it.” *Good ’Nuff Garage, LLC v. McCulley*, No. 3:21-cv-571, 2022 WL 4485810, at *12–13 (E.D. Va. 2022).

The decisions in *Good ’Nuff* and *Ticketmaster* are instructive. In *Good ’Nuff*, the defendant improperly accessed the plaintiff’s Facebook page, “posted on the Facebook page[,] and changed the contact email for the page.” 2022 WL 4485810, at *13. The court found that the defendant “obtained information” under the CFAA because he “had access to (and saw), at a minimum, settings pertaining to Plaintiff’s contact information and posts.” *Id.* Similarly, in *Ticketmaster*, the defendants improperly used automated programs, called “bots,” to “obtain[] tickets to events.” 315 F. Supp. 3d at 1174. The court found that the defendants “obtained information” under the CFAA because “(1) the tickets contain information on the face of the ticket . . . ; and (2) the tickets themselves are transmitted through the internet in the form of computer code, which is itself information.” *Id.*

Similarly, here, Entri obtained information by using user login information and accessing and altering DNS configuration settings, which are transmitted through GoDaddy’s API computer code and stored on GoDaddy’s servers. Specifically, Entri creates API keys that call to GoDaddy’s servers that manage DNS within GoDaddy’s systems. (Dkt. 105 ¶ 111.) Entri argues that it does not “collect information,” but admits that it “configure[s] [GoDaddy customers’] DNS settings,” which are stored within GoDaddy’s systems. (Dkt. 140 at 17; *see also* Dkt. 105 ¶¶ 21–22, 111–12.) Entri’s access to and observation of the data within GoDaddy’s systems and API constitutes “obtaining information” under the CFAA.

Entri’s argument that it obtained GoDaddy’s *customers’* data holds no weight because Entri obtained that data through GoDaddy systems. Indeed, courts often find liability under the CFAA where the defendant obtained information of a software company’s “users.” *See, e.g., Facebook*,

Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1068 (9th Cir. 2016) (defendant observed Facebook users’ data and pages, which were “stored . . . on [Facebook’s] physical servers”); *Microsoft Corp. v. John Does I-8*, No. 1:14-cv-811, 2015 WL 4937441, at *9 (E.D. Va. Aug. 17, 2015) (defendants’ “botnets” “extract[ed] . . . personal information from . . . [Microsoft’s] customers’ computers”); *Microsoft Corp. v. Does I-2*, No. 1:21-cv-822 RDA/IDD, 2022 WL 18359421, at *4 (E.D. Va. Dec. 27, 2022), *report and recommendation adopted*, 2023 WL 289701 (E.D. Va. Jan. 18, 2023) (defendants “gain[ed] unauthorized access to the Microsoft []365 credentials of Microsoft customers and their networks”).

Entri’s access to GoDaddy’s API and systems is thus sufficient to state a claim under the CFAA. *See Good ’Nuff*, 2022 WL 4485810, at *12–13 (stated claim where defendant “access[ed] . . . and saw” Plaintiffs’ Facebook “settings”); *Ticketmaster*, 315 F. Supp. 3d at 1174 (stated claim where defendant observed information on ticket and “computer code” that tickets were “transmitted through”).

3. GoDaddy Sufficiently Pled Damages

Entri argues that GoDaddy did not sufficiently plead damage or loss. Under the CFAA, GoDaddy must plead that, during any one-year period, it has suffered damage or loss “aggregating at least \$5,000 in value.” 18 U.S.C. § 1030(c)(4)(A)(i)(I). The CFAA defines “damage” as “any impairment to the integrity or availability of data, a program, a system, or information.” *Id.* § 1030(e)(8). And it defines “loss” as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” *Id.* § 1030(e)(11). GoDaddy suffered both damages and loss in excess of \$5,000 in value.

First, GoDaddy suffered damages as contemplated by the CFAA. The CFAA’s definition of “damage” includes “any diminution in the completeness or usability of the data on a computer system.” *Shah v. Rodino*, No. 3:13-CV-103-JD-CAN, 2015 WL 13942656, at *4 (N.D. Ind. June 26, 2015) (quoting *Farmers Ins. Exch. v. Auto Club Grp.*, 823 F. Supp. 2d 847, 852 (N.D. Ill. 2011)). Entri made numerous unauthorized API requests directed at GoDaddy’s systems. (Dkt. 105 ¶¶ 84–85.) Entri’s repeated unauthorized requests burdened GoDaddy’s servers and caused diminution in the usability of the data on those servers and, consequently, the platform’s performance. Discovery will reveal the extent of Entri’s activities on—and potential security threats to—GoDaddy’s data servers. (*See id.* ¶ 112 (“Entri improperly procured information and altered the configuration settings of domains registered with GoDaddy—domains that it was accessing without authorization.”).) Thus, dismissal based on purported lack of “damage” would be premature at this stage.

Second, GoDaddy suffered “loss” in excess of \$5,000 in value. The Fourth Circuit Court of Appeals held that the CFAA’s definition of “loss” is a “broadly worded provision” that includes “costs incurred as part of the response to a CFAA violation, including the investigation of an offense.” *Vanderhye*, 562 F.3d at 646 (collecting cases).

Here, GoDaddy incurred costs “in investigating and responding to the consequences of [Entri’s] unauthorized access,” which resulted in “damages of at least \$5,000.” (Dkt. 105 ¶ 113.) GoDaddy has taken—and continues to take—a variety of steps to address Entri’s unauthorized use of its API. For instance, GoDaddy had to “disconnect[] Entri from GoDaddy’s Domain Connect,” and then, upon continuing to receive substantial API calls, conducted further investigation to discover that Entri had in fact “managed to work around this disconnection.” (*Id.* ¶¶ 77, 113.) In response, GoDaddy dedicated resources to updating its API TOU “to prohibit Entri Connect from

using” its API. (*Id.* ¶¶ 72, 78.) Still, GoDaddy has not uncovered how Entri is overcoming its restrictions to access GoDaddy’s API, and GoDaddy has been unsuccessful in its efforts to prohibit Entri from doing so. (*Id.* ¶ 83.) Until GoDaddy can successfully prevent Entri from accessing its API, it will continue to suffer losses, including due to the “significant data processing and server costs” resulting from Entri’s unauthorized access. (*Id.* ¶¶ 77–84.)

In addition to investigating Entri’s unauthorized access, GoDaddy also incurred costs “investigating and responding to” the “posed security and operational threats to GoDaddy” caused by Entri’s unauthorized access. (*Id.* ¶ 113.) Indeed, without direct “oversight” into Entri’s “access and configur[ation] [of] domain[]” settings, GoDaddy has to dedicate resources to address these additional “security vulnerabilities.” (*Id.* ¶ 85.) If GoDaddy were to ignore these increased vulnerabilities, it would “risk that its customers will fault GoDaddy if,” for example, “Entri is compromised by a security incident.” (*Id.* ¶ 92.)

GoDaddy’s allegations of loss and explanation that the losses resulted in more than \$5,000 of value is sufficient under the CFAA. *See Vanderhye*, 562 F.3d at 645–46 (pleadings that university “feared the possibility of a technical glitch in [their] system and concluded an investigation was necessary . . . to determine what happened,” resulting in “numerous man-hours . . . spen[t] responding to” defendant’s unauthorized access, was loss “plainly contemplate[d]” by the CFAA); *Space*, 306 F. Supp. 3d at 852–53 (pleading costs of “conducting a damage assessment and convening and communicating with [third parties] regarding the alleged breach,” which plaintiff alleged exceeded “\$5,000 in value during a one-year period,” was sufficient “loss”); *Microsoft Corp. v. Does*, No. 1:19-cv-01582, 2020 WL 13894281, at *6 (E.D. Va. Nov. 20, 2020) (efforts to “block[]” defendants’ attempts to use software and “prevent the misperception that Microsoft is the source of the damage” sufficient injury).

Entri argues that GoDaddy does not allege loss “with specificity.” But Entri misplaces reliance on cases where the plaintiff failed to make *any* factual allegations of loss. *See, e.g., Phoenix Co., Inc. v. Castro-Badillo*, No. 23-1371 (RAM), 2024 WL 3742368, at *8 (D.P.R. Aug. 9, 2024) (plaintiff did not allege “what investigative measures were taken,” or “what damage, if any, was actually caused by the hacking, and simply states there was an ‘interruption of service’ without alleging facts as to what” services were interrupted). As discussed above, GoDaddy specifically alleged what type of loss it incurred.

Entri also argues that GoDaddy’s “loss” is insufficient because it did not result in interruption of service or impairment of the protected computer. But its cited cases do not hold that Entri’s actions must “cause[] an[] interruption of service,” as Entri contends. (Dkt. 140 at 22.) Rather, they hold that, to recover costs relating to investigations or efforts to block a defendant, those efforts must be related to potential damage, interruption, or impairment caused by defendant’s access. *See, e.g., William Gottlieb Mgmt. Co., LLC v. Carlin*, No. 20 Civ. 08907 (VM), 2024 WL 1311854, at *4 (S.D.N.Y. Mar. 26, 2024) (plaintiff’s “investigation” merely confirmed that defendant “accessed its data,” which plaintiff already knew); *CoStar Grp., Inc. v. Leon Cap. Grp., LLC*, No. 21-cv-2227 (CRC), 2023 WL 5133182, at *4 (D.D.C. Aug. 10, 2023) (plaintiff failed to allege “that it expended resources responding to ‘technological harms’ caused by [defendant’s] unauthorized use”); *Civic Center Motors, Ltd. v. Mason Street Import Cars, Ltd.*, 387 F. Supp. 2d 378, 382 (S.D.N.Y. 2005) (“[C]osts not related to computer impairment or computer damages are not compensable under the CFAA.”). And here, GoDaddy has alleged that its costs result from “investigating and responding to the consequences of [Entri’s] unauthorized access” and the “posed security and operational threats to GoDaddy.” (Dkt 105 ¶ 113.) Such allegations align with the case law.

Indeed, the Fourth Circuit Court of Appeals has emphasized that the definition of “loss” under the CFAA is “broadly worded” and includes “costs incurred as part of the response to a CFAA violation, including the investigation of an offense.” *Vanderhye*, 562 F.3d at 645–46 (investigation “to determine what happened” was loss “plainly contemplate[d]” by the CFAA). And several courts have held that the “cost of ‘responding to an offense,’ on its own, qualifies as loss under the CFAA, without any need to connect it to an interruption of service.” *Ticketmaster*, 315 F. Supp. 3d at 1172; *see also Patrick Patterson Custom Homes, Inc. v. Bach*, 586 F. Supp. 2d 1026, 1036 (N.D. Ill. 2008) (response costs “are recoverable regardless of whether there is an interruption of service, and courts have sustained actions based on allegations of costs to investigate and take remedial steps in response to a defendant’s misconduct”); *Facebook*, 844 F.3d at 1066 (holding that “employees spen[ding] many hours, totaling more than \$5,000 in costs, analyzing, investigating, and responding to [defendant]’s actions” constituted loss).

GoDaddy has thus sufficiently alleged that Entri violated the CFAA.

IV. CONCLUSION

GoDaddy repeatedly made Entri aware of GoDaddy’s prohibitions on Entri’s access and use of GoDaddy’s systems and API software. Despite knowing that its actions were prohibited, Entri continued its course of conduct. GoDaddy clearly alleged that Entri’s actions caused GoDaddy to incur monetary damages and created security risks. GoDaddy never provided Entri carte blanche access to GoDaddy’s systems and API software. GoDaddy respectfully requests that the Court deny Entri’s Motion to Dismiss so that Entri can be held accountable for its violations. In the alternative, GoDaddy respectfully requests leave to amend its counterclaims to fully detail Entri’s misconduct and the harm it causes.

Dated: December 6, 2024

Respectfully submitted,

/s/ Douglas J. Dixon

Douglas J. Dixon (pro hac vice)
Andrew K. Walsh (pro hac vice)
Justin M. Greer (pro hac vice)
Erik C. Savitt (pro hac vice)
Hueston Hennigan LLP
620 Newport Center Dr., Suite 1300
Newport Beach, CA 92660
Phone: (949) 229-8640
Fax: (888) 866-4825
ddixon@hueston.com

/s/ Chad E. Kurtz

Chad E. Kurtz
VA Bar No. 88863
COZEN O'CONNOR
2001 M Street, NW, Suite 500
Washington, D.C. 20036
Tel: (202) 463-2521
Fax: (202) 640-5939
ckurtz@cozen.com

*Attorneys for Defendant GoDaddy.com,
LLC*

CERTIFICATE OF SERVICE

I hereby certify that on December 6, 2024, a true and correct copy of the foregoing was served using the Court's CM/ECF system, with electronic notification of such filing to all counsel of record.

/s/ Chad E. Kurtz
Chad Kurtz
*Attorney for Defendant GoDaddy.com,
LLC*